Security Frame Work against Denial of Service Attacks in Wireless Mesh Networks

A thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Technology

in

Information Security

by

Prasoon P S

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela, Orissa, 769 008, India

May 2011

Security Frame Work against Denial of Service Attacks in Wireless Mesh Networks

A thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Technology

in

Information Security

by

Prasoon P S
(209cs2092)

under the guidance of

Prof. Bibhudatta Sahoo

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Orissa, India

May 2011

To my parents and friends

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Orissa, India.

Certificate

This is to certify that the work in the thesis entitled ***Security Frame Work Against Denial of Service Attacks in Wireless Mesh Networks*** by ***Prasoon P S*** in partial fulfillment of the requirements for the award of the degree of Master of Technology in Information Security during session 2010-2011 in the department of Computer Science and Engineering, National Institute of Technology Rourkela is an authentic work carried out by him under my supervision and guidance. To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other University/Institute for the award of any Degree or Diploma.

Place: NIT Rourkela
Date: 20 May 2011

Prof. Bibhudatta Sahoo
Assistant Professor
Dept. of Computer Science & Engineering
National Institute of Technology
Rourkela-769 008, Odisha (India)

Acknowledgment

First, I would like to express my heartfelt gratitude to my supervisor Prof. Bibhudatta Sahoo for his guidance, encouragements, immense patience and support throughout my research at the National Institute of Technology, Rourkela. He helped me in finding research topics, proposing solutions and verifying results. Without his endless efforts, knowledge, patience, and advices, this research would have never been possible. It has been a great honor and pleasure for me to do research under his supervision.

I would like to thank Dr. Ashok Kumar Turuk, Head of the Department, Computer Science engineering, National Institute of Technology, Rourkela for his support during my work.

I am also thankful to all other Professors and faculty in Department of Computer Science and Engineering, National Institute of Technology, Rourkela for giving encouragement during my thesis work.

I would like to thank all of my colleagues and friends for their inspiration and help.

I thank all the members of the Department of Computer Science and Engineering, and the Institute, who helped me by providing the necessary resources, and in various other ways, in the completion of my work.

I would like to thank my parents for their encouragement and love.

Prasoon P S

Abstract

Wireless mesh networks (WMNs) are emerging as a solution for large scale high speed internet access through their scalability, self configuring and low cost. But as compared to wired networks, WMNs are largely prone to different security attacks due to its open medium nature, distributed architecture and dynamic topology. Denial of service (DoS) attacks is one of the most common types of attack which is possible in WMNs. DoS attacks are most common in networks which connect to internet and since WMNs are mainly designed for fast and long distance internet access this type of attacks are common in the network. In our work we mainly concentrate our study on two denial of service attacks namely gray hole attacks (a.k.a selective forwarding attacks) and black hole attacks. Wireless mesh networks consist of both mesh routers and mesh clients. We confine our studies to mesh routers which are stationary. We implement both gray hole attack and black hole attack in mesh routers and study the delivery ratio of the network with and without the presence of attack routers. By simulating the scenario with AODV protocol we studied the delivery ratio of packets and find out how it is affecting the network in the presence of an attack router. After studying the results we propose a new detection algorithm based on overhearing the neighboring node to which the packet is forwarded. By keeping the history of number packets forwarded and the number of packets overheard the algorithm determines the number of packets dropped and determines the probability of attack. This probability is checked with the threshold value of probability and determines whether a router is misbehaving or not. We also considered the possibility of false positives and took necessary measures in the algorithm to reduce it. If a router is found misbehaving it is removed from the network and excluded from further forwarding of packets. We analyze our algorithm in the presence of an attack router and detect the attack router and study the improvement in the delivery ratio. Through simulation we evaluate the performance of our algorithm depending on the packet delivery ratio achieved and time.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Introduction

Thesis Organization

Chapter 1

Introduction

1.1 Introduction

Wireless mesh networks (WMNs) are a multi-hop wireless communication among different nodes are dynamically self-organized and self-configured, with the nodes in the network automatically establishing an ad-hoc network and maintaining the mesh connectivity. WMNS are emerged as a promising concept to meet the challenges in wireless networks such as flexibility, adaptability, reconfigurable architecture etc [1]. WMNs consist of two kinds of nodes: mesh routers and mesh clients. Mesh routers are routers which forms the stationary or least mobile part of the mesh network with less power constraint and forms the backbone of the mesh network. Mesh clients are nodes which are mobile in the network with power constraints. Though mesh clients can also do routing by forwarding packets to the next node in mesh networking the hardware and software platform for them are much simpler compared to mesh routers. Mesh routers can do all the gateway/bridge functions as in conventional wireless router, in addition to that it contains additional functions to support mesh routing. They can support multiple wireless interfaces built on either the same or different wireless access technologies. Thus mesh routers are dedicated and stationary nodes for routing functions with less power constraint. Mesh clients are nodes with no gateway/bridge functions and only one wireless interface is needed in mesh clients. Wireless mesh networks can be integrated with other networks because of the bridge/gateway functions provided by the mesh router. The presence of mesh routers and hop by hop

forwarding in WMNs bring many advantages compared to conventional ad-hoc network such as low up-front cost, higher scalability, easy network maintenance, robustness, reliable and need less transmission power.

A wireless mesh network enables ad-hoc mode peer to peer interconnection among mesh clients are is called client meshing [1]. With client meshing, mesh routers that stay outside the radio coverage of a mesh router can rely on other intermediate clients to relay packets to them to get WMN access network connections. Thus packets from a mesh client which lies far away from the mesh router has to travel multi hop client-to-client and client-to-router wireless link before reaching its destination. The number of hops is determined by the geographical location of the client and also the organization structure of the access network. The architecture of wireless mesh networks can be classified in to three main groups based on the functionalities of the nodes namely infrastructure/backbone WMNs, client WMNs and Hybrid WMNs. In infrastructure WMNs wireless mesh routers will form a mesh of self-configuring, self healing links among themselves. With gateway functionality these routers can be connected to the internet. This approach provides backbone for conventional clients and enables integration of WMNs with existing wireless networks, through gateway/bridge functionalities in mesh routers. In client meshing the client devices will form a mesh to perform routing and configuration functionalities as well as providing end-user applications to users. In this architecture no mesh routers are present and thus are same as the conventional ad-hoc network. Hybrid WMNs is the combination of infrastructure and client meshing and a mesh network is formed between the clients and as well as the routers. Mesh clients can access the network through mesh routers as well as directly meshing with each other.

Because of the self configurable architecture of wireless mesh networks and the wide usage of WMNs for accessing internet, mesh routers and clients are prone to different type of security issues. So providing solution to the security challenges is a major research area in recent years in the fields of WMNs. WMNs are facing two broad categories of attacks such as passive attacks and active attacks. In the case

of passive attack, the attackers simply analyze and listen to the network traffic with the objective of capturing sensitive information which can be used later to launch an active attack on the network [2]. Active attacks are which will directly damage the network bandwidth either by tampering, modification or just by dropping of packets. Because of the multi hop nature and ad-hoc connectivity, WMNs are prone to both kinds of these attacks. The three important features of a secure network are confidentiality, integrity and service availability. Confidentiality is compromised by passive attacks, integrity by active attacks and availability by the most severe form of active attack on internet namely Denial of Service (DoS) attacks. Since WMNs is mainly used in long distance internet access and other applications which uses internet, DoS attack is treated as the highest security risk for this network, as DoS uses internet as a platform to be launched.

Denial of Service is one of the major issues of all types of wireless mesh networks as it is mainly designed for internet access . When authorized users are not provided a request service within a defined maximum interval of time, it means that a DoS violation has occurred. It is the most harmful and dangerous attack which can be launched any layer of wireless mesh networks. DoS attack can be launched in physical layer by radio jamming a device, in MAC layer by sending bulk MAC control messages to an innocent neighbor or by holding the MAC channel for unnecessary continuous transmission. Network layer is highly vulnerable to different DoS attacks due to multi-hop routing, as the number of hop increases the routing overheads increase. DoS attack in network layer can affect the routing mechanism or can degrade the network performance by exhausting the network resources. A DoS attack in network layer can be black hole attack in which a malicious node absorbs all the packets forwarded towards the target node and dropping those packets or dropping all the packets go through the malicious node. Another form of attack is the selective dropping attack or gray hole attack in which the malicious node selectively dropping some packets or randomly dropping some packets. Worm hole attack is another form of attack which will create networking disruptions. Another for DoS attack in network layer called the flooding attack in

which the attacker transmits a flood of packets to the target node or to congest the network and degrade its performance [2].

In our study we deal with two types of denial of service attacks in network layer namely black hole attacks and gray hole attacks and propose a defense mechanism for detecting and eliminating the attacks. In our work we concentrate our study on the mesh routers alone which are the stationary part of WMNs. We implemented the two attacks in Ad-hoc On-Demand Distance Vector (AODV) protocol and studied the impact of these attacks in the network. The protocols implemented are considering attacks on the data packets passed and forward the control packets without dropping. Simulation of the attack is done in ns-2.34 (network simulator 2). Although ns-2.34 contains the AODV protocol, there were no modules available to implement the malicious nodes. So we modified the AODV protocol to implement gray hole and black hole attack and added as a new protocol to ns-2.34. After implementing both black hole and gray hole attack as new two protocols we studied the network performance with the presence of attack node and without that. As expected the network performance of the network degrades in the presence of attack node. Afterwards we proposed a solution for eliminating the attack nodes from the network based on a detection algorithm. The algorithm is based on overhearing the neighboring nodes and observing the forwarding behavior of the nodes. For overhearing the neighboring nodes the AODV protocol should be in promiscuous mode in which the router can over hear the data forwarded by the neighboring nodes. Since promiscuous mode is not implemented in ns-2.34 we evaluated our algorithm by implementing in perl language and analyzing the trace files obtained during the gray hole and black hole attack simulation. Simulation result shows that our solution eliminates the attacker nodes from the network and there by improving the delivery ratio of the network.

1.2 Thesis Organization

In chapter 2 we presented wireless mesh networks and also the three different architectures and their vulnerabilities to denial of service attacks including black

hole and gray hole attack. We also present the different routing metrics which are used in WMNs. In chapter 3 we described AODV protocol in detail and how gray hole attack and black hole attack makes the protocol to misbehave and also described how the new protocols supporting attacks are implemented in ns-2.34. In chapter 4 we explains our proposed algorithm to detect and eliminate the attacks and also the simulation and evaluation of the algorithm and the results obtained.

Finally Chapter 5 discusses the concluding remarks and future research work.

Chapter 2

Background

Wireless Mesh Networks

Network Architecture

Routing Metrics for WMNS

Routing protocols in WMNS

Security Challenges in Wireless Mesh Networks

Denial of Service attacks in Network layer of WMNS

Chapter 2

Back ground

2.1 Wireless Mesh Networks

Wireless Mesh Network is a promising wireless technology for several emerging and commercially interesting applications, e.g., broadband home networking, community and neighborhood networks, coordinated network management, intelligent transportation systems. It is gaining possible attention as a possible way for Internet service providers and other end-users to establish robust and reliable wireless broadband service access at a reasonable cost. Different from traditional wireless networks, nodes in WMN automatically establish and maintain network connectivity. This feature brings many advantages for the end-users, such as low up-front cost, easy network maintenance, robustness, and reliable service coverage [3]. The gateway and bridge functionalities in mesh routers enable the integration of wireless mesh networks with various existing wireless networks, such as wireless sensor networks, wireless-Fidelity (Wi-Fi), and WiMAX [1]. Some of the characteristics of wireless mesh networks are as follows:

- **Increased Reliability**

  In WMNs the wireless mesh routers provide multiple paths between the sender and receiver of the wireless connection. This eliminates single point failures and potential bottleneck links, which increases the communication reliability. Some of the common problems in wireless networks such as node failures, path failures etc can be over come by the presence of multiple paths.

Thus WMN operates reliably over an extended period of time even in the presence of these failures.

- **Low Installation Costs**

  In a wireless network, if we want to provide full coverage in a metro scale area to provide internet connection a large number of access points (APs) are required and each of these APs should be connected to internet through a wired connection. The main draw back of this solution is of high infrastructure costs, because an expensive cable connection is required to the wired internet backbone. WMN reduces this infrastructure costs in which only a few points is required to connect to the wired network and the other routers will access the network through those which are connected. So implementation of WMN can be made fast in the presence of less wired points and also the network can be modified at a reasonable cost.

- **Large Coverage Area**

  One of the disadvantages of wireless LANs is that for a specific transmission power, the coverage and connectivity of WLANs decreases as the distance of the end user from the access point increases. On the other hand, the multi hop and multi channel communication provided by WMNs increases the coverage and connectivity of wireless mesh networks without much performance degradation [1].

- **Automatic Network Connectivity**

  Wireless mesh networks are dynamically self-organized and self-configured, in other words mesh clients and mesh routers automatically establish network connectivity. For example when new nodes are added into the network, those nodes utilize their meshing functionalities to automatically discover all possible mesh networks and determine the optimal paths to the wired

internet [1]. Moreover the existing mesh routers reorganize the network considering the newly available routes and hence the network can be easily expanded.

In this chapter we present survery about the different architectures of WMNs, routing metrics which are used in different routing protocols in WMNs followed by routing protocols, and finally the security vulnerabilities in different layers in the WMNs due to Denial of Service attacks with concentrating our study mostly on DoS attacks in the network layer of wireless mesh networks.

2.2 Network Architecture

As mentioned in chapter 1, the architectures in wireless mesh network can be classified in to three different types.

2.2.1 Infrastructure/Backbone WMNS

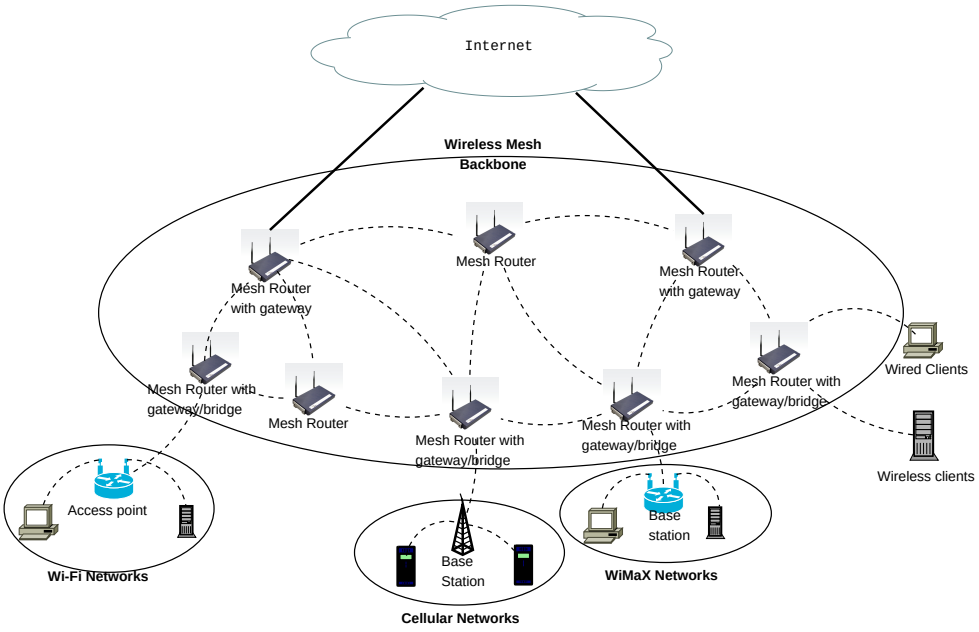

Figure 2.1: Infrastructure/backbone WMNS

In this architecture the mesh routers in WMNs are connected and form a mesh and will provide an infrastructure for clients, as shown in Fig. 2.1 , where

solid lines indicates wired link where as dashed lines indicate wireless links. The backbone routers can be built using different radio technologies in addition to the mostly used IEEE 802.11 technologies [1]. The mesh routers form a self-configuring and self-healing mesh among themselves. With gateway function few of the mesh routers will be connected to the internet. The conventional clients with an Ethernet interface can connect to any of the mesh routers through the Ethernet interface to communicate with others or to access the internet. These routers form a meshing known as infrastructure meshing which acts as an infrastructure to the client nodes. Clients having the same radio technology as the routers can connect directly to them others have to send packets to their access points or base stations which will be connected to the routers through the gateway for internet access. This approach enables integration of WMNs with existing wireless networks and also provides a backbone for conventional clients.

2.2.2 Client WMNS

In this architecture clients form a mesh network among themselves and no routers exist. The clients will establish peer-to-peer networks among them and constitute the actual network performing routing and configuration functions as well as providing end-user applications to costumers. The clients will communicate using a single radio interface among the devices and a packet is forwarded to destination by hopping through the device. Thus, a Client WMNs is same as the conventional ad-hoc network. By comparing with the Infrastructure WMNs the requirements on the clients increased in Client WMNs because the end-users must perform additional functions such as routing and self-configuration.

2.2.3 Hybrid WMNS

Hybrid WMN is a combination of both Infrastructure and Client WMN in the sense that both the routers and clients will form mesh networking [1]. Routers will form the backbone by meshing each other and the clients can form mesh network among themselves for communicating hop-by-hop each other and to connect to the backbone router. Thus mesh clients can access the network through mesh

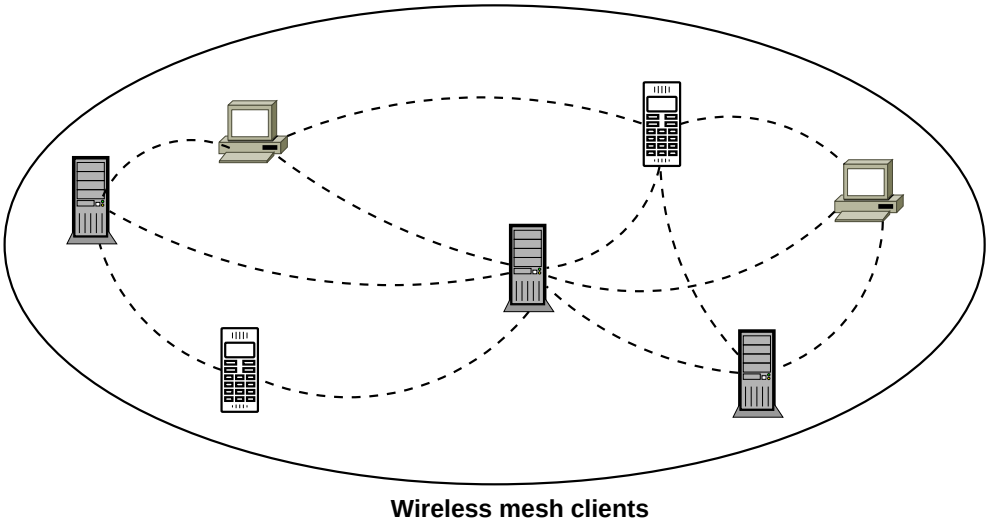

Figure 2.2: Client WMNS

routers as well as meshing with other mesh clients. While the meshing of routers to form backbone network will provide connectivity to other networks such as internet, Wi-Fi, WiMaX, cellular and sensor networks, the routing capability of mesh clients will provide improved connectivity and coverage inside the WMNs.

Since from our study of different architectures we can see that hybrid WMNs has all the advantages of a wireless mesh network, the characteristics of WMNs are outlined according to this architecture as stated in [1]are:

- WMNs support ad hoc networking and have the capability of self-forming, self-healing and self-organization.
- WMNs are a multi-hop wireless networks like ad-hoc networks, but with a wireless backbone network provided by mesh routers.
- Mesh routers have minimum mobility or stationary and are dedicated to routing and configuration, which reduces the load of mesh clients and other

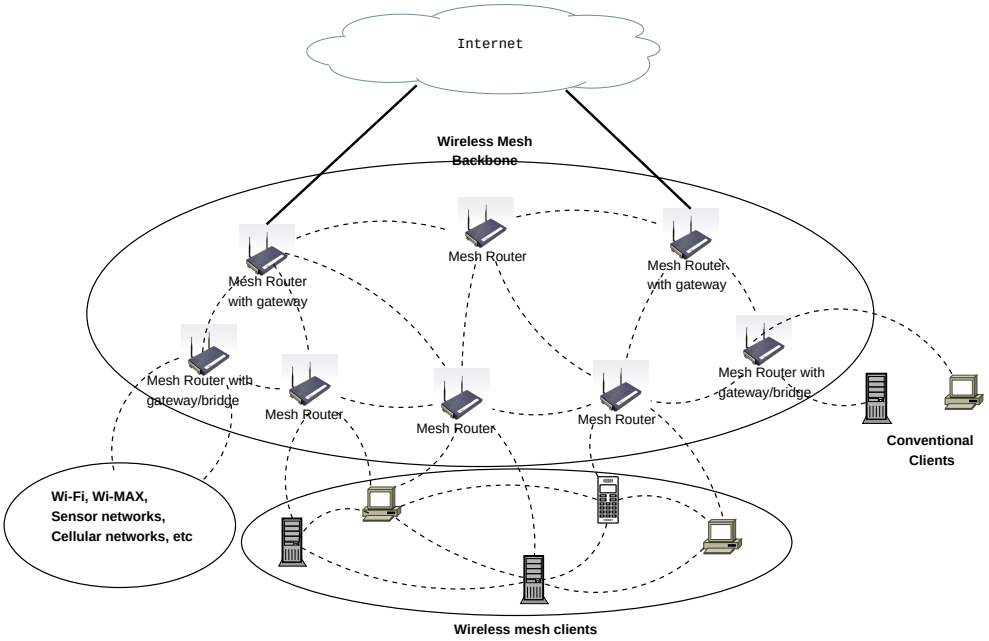

Figure 2.3: Hybrid WMNS

nodes.

- Mobility of end nodes is supported through the wireless infrastructure.
- Mesh routers integrate heterogeneous networks including both wired and wireless networks and thus multiple type of network access exist in WMNs.
- Power consumption constraints are different for mesh routers and mesh clients.
- WMNs are not stand-alone and need to be compatible and interoperable with other networks.

2.3 Routing Metrics for WMNs

Most of the ad hoc routing protocols use hope count as a routing metric. In the early stages these routing metrics are also used in WMNs. These assume that the link in the path work properly or not work at all and consider all links of equal bandwidth. So in this case minimizing the hop count will reduce the packet delay and also increases the throughput. But in wireless mesh networks links are

not of equal bandwidth. A minimum hop count path has higher average distance between nodes present in that path compared to a higher hop count path. This reduces the strength of the signal received by the nodes in that path and thereby increases the loss ratio at each link. Hence, it is always possible that a two-hop path with good link quality provides higher throughput than a one-hop path with a poor/lossy link. The wireless links usually have asymmetric loss rate. Hence, new routing metrics based on the link quality like ETX (Expected Transmission Count), per-hop RTT (Round-Trip Time), and per-hop packet pair is proposed [4].

- **Expected Transmission Count (ETX)**

  The metric ETX is defined as the expected number of transmissions (including retransmissions) needed to successfully deliver a packet over a link. A successful transmission requires acknowledgment back to the sender. ETX considers transmission loss probability in both directions, which may not be equal. The multi-radio multi-channel architecture is used in WMNs to improve the throughput. In this case the routing metric based on link quality alone is not sufficient. It should also consider the channel diversity on the path. To achieve this new routing metric WCETT (Weighted Cumulative Expected Transmission Time) is proposed.

- **Weighted Cumulative Expected Transmission Time (WCETT)**

  WCETT takes both link quality and channel diversity into account. The link quality is measured by a per-link metric called Expected Transmission Time (ETT). ETT is the expected time to transmit a packet over a link. The WCETT metric takes into consideration the quality of links and the intra flow interference along the path. But it fails to take into account inter flow interference on the path. Thus, another routing metric MIC (Metric of Interference and Channel switching) is proposed for multi-channel multi-radio WMNs to overcome this drawback.

- **Metric of Interference and Channel Switching (MIC)**
  MIC considers the quality of links; inter flow interference, and intra flow interference. This metric is based on Interference-Aware Resource Usage (IRU) and Channel Switching Cost (CSC) metrics. IRU captures the differences in the transmission rate and the loss ratios of the wireless link and the inter flow interference.

2.4 Routing Protocols in WMNs

All the routing protocols available for the prior works in wireless networks especially multi-hop ad hoc networks work well for wireless mesh networks. Thus the protocols designed for ad-hoc networks such as Ad-hoc On-demand Distant Vector Protocol (AODV), Dynamic Source Routing (DSR), and Destination Sequence Distant Vector routing (DSDV) works well with wireless mesh networks too. Since we are using AODV protocol for implementing gray hole attack in WMNs we will discuss about this protocol in detail in Chapter 3. Here we will discuss some of the protocols which are exclusively designed for wireless mesh networks by taking into consideration of the routing metrics we discussed. Since wireless mesh networks use two antennas for transmitting and receiving packets as compared to one antenna in ad hoc networks and also the link quality between different nodes in the network are not the same and to make advantage of meshing, new routing protocols are designed to improve the routing quality of WMNs. Also the routers in wireless mesh network have minimal mobility and there is no power constraint and the clients are mobile with limited power. Hence the links in wireless mesh networks are long lived compared to the links in ad-hoc networks. Since two types of nodes present in WMNs, that is the mesh routers and mesh clients some protocols even follow different routing techniques for routers and clients.

2.4.1 Link Quality Source Routing (LQSR)

LQSR is based on DSR and uses ETX as the routing metric. The main difference between LQSR and DSR is getting the ETX metric of each link to find the path.

DSR is modified in several ways to support routing according to link-quality metrics. This includes modifications to Route Discovery and Route Maintenance and new mechanisms for Metric Maintenance. During the route discovery phase, the source node sends a Route Request (RREQ) packet to neighboring nodes. When a node receives the RREQ packet, it appends its address to the source route and the ETX value of the link in which the packet was received. The destination sends the Route Reply (RREP) packet with a complete list of links along with the ETX value of those links [4]. LQSR also propagates the ETX value of the links during the data transmission phase as the link quality varies with time.

LQSR uses a reactive mechanism to maintain the metrics for the active links. When a source-routed packet is sent, each intermediate node updates the source route with the current metric for the next link. This carries up-to-date link metrics forward along with the data. To get the link metrics back to the source of the packet flow (where they are needed for routing computation), the recipient of the packet sends a Route Reply back, conveying the up-to-date link metrics from the arriving Source Route. This Route Reply is delayed up to one second because of waiting for a piggy-backing opportunity.

LQSR uses a proactive background mechanism to maintain the metrics for all links. Occasionally each LQSR node sends a Link Info message. The Link Info contains current metrics for each link from the originating node. The Link Info is piggy-backed on a Route Request. Hence it floods throughout the neighborhood of the node. LQSR piggy-backs Link Info messages on all Route Requests if possible. The link metric support also affects Route Maintenance. When Route Maintenance notices that a link is not functional (because a requested Ack has not been received), it penalizes the link's metric and sends a Route Error. The Route Error carries the links updated metric back to the source of the packet.

2.4.2 Multi-Radio Link Quality Source Routing (MR-LQSR)

MR-LQSR is a new routing protocol for multi-radio multi-channel WMNs. It uses WCETT as the routing metric. MR-LQSR is a combination of the LQSR protocol and the WCETT metric. The neighbor node discovery and propagating the link

metric to other nodes in the network in MR-LQSR is like in the DSR protocol. But assigning the link weight and finding the path weight using the link weight are different from DSR [4]. The main difference is that DSR uses equal weight to all links in the network and implements the shortest path routing whereas MR-LQSR uses a WCETT path metric to find the best path to the destination.

2.4.3 Load and Interference Balanced Routing Algorithm (LIBRA)

A WCETT routing metric is used in a link state routing protocol does not satisfy the isotonicity property of the routing protocol and leads to formation of routing loops. To avoid the formation of routing loops by the routing metrics, LIBRA is proposed. LIBRA uses MIC as the routing metric [4]. In this, a virtual network is formed from the real network and decomposes the MIC metric into isotonicity link weight assignment on the virtual network. The objective of MIC decomposition is to ensure that LIBRA can use efficient algorithms such as Bellman-Ford or Dijkstra's algorithm to find the minimum weight path on the real network without any forwarding loops.

2.5 Security Challenges in wireless mesh networks

The main features of a secure wireless mesh network are [5]:

- Confidentiality
- Integrity
- Availability

The concept of confidentiality is the assurance that sensitive data is being accessed and viewed only by only those who are authorized to view it. Confidentiality implies that data is protected form breaches from unauthorized persons and the damage that would be done to the organization, person or government bodies due

to such breaches. The concept of integrity ensures that the data is not altered during the transfer from sender to receiver. Integrity guarantees that a message sent is the message received and the message is not altered intentionally or unintentionally. Availability ensures the survivability of network services despite attacks. The assurance of availability is very much a security issue. Long term Denial of Service attacks can seriously hinder the network performance.

Wireless mesh networks are facing two categories of threats [2]:

- Passive attacks and
- Active attacks

In passive attacks, objective of the attacker is to capture sensitive information of the target. The attackers simply analyze and listen to the network traffic with the objective to capture sensitive information of the target. These kinds of attacks compromise the confidentiality of the end user traffic. the unauthorized user gain illegal access to the network traffic without modifying the traffic. Passive attacks are very difficult to detect, as such attacks do not harm the user traffic or normal network operations. However, most of the passive attacks are later used for launching active attacks, as successful passive attack gain information related to the target users, network topology, traffic pattern etc. Such information can later be used for launching active or DoS attack. Passive attacks can be eavesdropping or traffic analysis. WMN is more vulnerable to passive attacks as compared to other wireless networks because of its multi hop nature and client nodes may have direct ad-hoc connectivity and relay traffic for one another [2], [6]. Active attacks can harm the network traffic either by tampering, modifications or dropping the packets, can reduce bandwidth or produce jitter in transmission and reduce through put. In case of active attacks also WMN is more vulnerable compared to other wireless networks because of multi hop architecture and ad-hoc connectivity. Multi-hop nature not only reduces bandwidth but also increases the routing overheads which can be exploited by the attackers to launch active attacks on WMNs. DoS attack is the most severe kind of wireless mesh attack.

Confidentiality is mostly encountered by passive attacks; integrity is threatened by active attacks, while availability of the broadband wireless networks are compromised by the most severe form of active attack, i.e. Denial of Service (DoS) attacks [6].

2.5.1 Denial of Service attacks in Wireless Mesh Networks

Denial of Service (DoS) is one of the major issues of wireless mesh networks as it is mainly designed for broadband internet access. When authorized users are not provided a requested service within a defined maximum waiting time, it means that a DoS violation has occurred [2]. It is the most harmful and dangerous attack which can be launched on any layer of broadband Wireless Network. DoS attacks prevent communication between network devices or a single device from sending or receiving traffic targeting availability. Availability ensures that authorized users can access the data, services and network resources from anywhere anytime.

- **Physical layer vulnerabilities**

  WMN uses the unlicensed 2.4GHz frequency band at physical layers. Physical layer can be made unavailable by a radio jamming device or a source noise to interfere these layers. This kind of attack can be detected using radio analyzers. However it is difficult to implement as it requires specialized hardware. In WMN, jamming attack can be launched from anywhere in the mesh network.

- **Link layer vulnerabilities**

  The WMN MAC uses shared medium among the nodes and is highly vulnerable to selfish attack and collisions. The selfish attack improves the bandwidth, throughput and QoS of the selfish node at the cost of another node. RTS/CTS can be compromised for MAC layer DoS attack either by sending bulk of MAC control messages to an innocent neighbor or by holding the MAC channel for unnecessary continuous transmission keeping an innocent

node back-off.

- **Network layer vulnerabilities**

  Network layer is highly vulnerable to different DoS attacks due to multi-hop environment. As the number of hops increase the routing overheads increase. DoS attacks at this layer can seriously disrupt the routing mechanism or can degrade the network performance by exhausting network resources. The network layer DoS attacks in WMN can be black hole attack, gray hole attack, worm hole attack and flooding attack [2], [7]. In Black hole attack, the malicious node absorbs all the traffic going towards the target node and drops the packets. In Gray hole attack, the malicious node selectively forwards the packets to the destination node while dropping the other packets. Worm hole attack will create routing disruptions. In flooding attack, the attacker transmits a flood of packets toward a target node and congests the network and degrades its performance. Flooding DoS attacks are difficult to handle. All these attacks are there in WMNs because of its multi hop nature.

2.6 Denial of Service attacks in Network layer of WMNS

- Rushing attacks

  Rushing attacks targeting the on-demand routing protocols were amongst the first exposed attacks on the network layer of multi-hop wireless networks. These attacks exploit the route discovery mechanism of on-demand routing protocols. In these protocols, the node requiring the route to the destination floods the Route Request message, which is identified by a sequence number [7]. To limit the flooding, each node only forwards the first message that it receives and drops remaining messages with the same sequence number. To avoid collusion of these messages, the protocols specify a specific amount of delay between receiving the Route Request message by a particular node

and forwarding it. The malicious node launching the rushing attack forwards the Route Request message to the target node before any other intermediate node from source to destination. This can be easily achieved by ignoring the specified delay .

- Worm hole attacks

  A wormhole attack's objective is similar to rushing attack but the technique used is different. During a wormhole attack, two or more malicious nodes collude together by establishing a tunnel using an efficient communication medium (wired connection or high-speed wireless connection, etc.). During the route discovery phase of on-demand routing protocols, the Route Request messages are forwarded between the malicious nodes using the tunnel [8]. Therefore, the first Route Request message that reaches the destination node is the one forwarded by the malicious node. Consequently, the malicious nodes are added in the path from source to destination. Once the malicious nodes are included in the routing path, the malicious nodes either drop all the packets, resulting in complete denial of service, or drop the packets selectively to avoid detection.

- Black hole attacks

  A black hole attack (or sink hole attack) also leads to denial of service in wireless mesh networks. It also exploits the route discovery mechanism of on-demand routing protocols. In a black hole attack, the malicious node always replies positively to a Route Request even if it may not have a valid route to the destination. Because the malicious node does not check its routing entries, it will always be the first to reply to the Route Request message [9]. Hence almost all the traffic within the neighborhood of the malicious node will be directed towards the malicious node, which may drop all the packets, resulting in denial of service [10].

- Gray hole attacks

  A gray hole attack is a variant of the black hole attack. In a black hole attack, the malicious node drops all the traffic that it is supposed to forward. This may lead to possible detection of the malicious node [11], [12]. In a gray hole attack, the packets are dropped selectively, thus avoiding the detection. A gray hole attack does not lead to complete denial of service, but it may go undetected for a longer duration of time. This is because the malicious packet dropping may be considered as congestion in the network [13]. This also leads to selective packet loss.

- Sybil attacks

  In a Sybil attack, a malicious node creates multiple identities in the network, each appearing as a legitimate node. WMNs are supposed to take advantage of the path diversity in the network to increase the available bandwidth and reliability. But if the malicious node creates multiple identities in the network, the legitimate nodes will add these identities in the list of distinct paths available to a particular destination, assuming these identities to be distinct network nodes [2]. When the packets are forwarded to these fake nodes, the malicious node that created the identities processes these packets. Consequently, all the distinct routing paths will pass through the malicious node. The malicious node may then launch any of the above-mentioned attacks. Even if no other attack is launched, the advantage of path diversity is diminished, resulting in performance degradation.

Chapter 3

Gray hole and Black hole attacks

Ad-hoc On-demand Distant Vector (AODV) routing protocol

Black hole attacks

Gray hole attacks

Implementing the new protocol in NS-2 which shows Gray hole behavior

Implementing Black hole behavior

Chapter 3

Gray hole and Black hole attacks

In this work we focus our attention to two special type of Denial of Service (DoS) attacks called gray hole attack or selective dropping attack and black hole attack or sink hole attack. We consider these attacks on the less mobile or almost stationary wireless mesh routers. Gray hole attack is a type of attack in which the attack router accepts the packets and refuses to forward certain packets by just dropping the packets. In black hole attack the attack router will advertise in the network that it has a fresh route to the destination and after that may drop all the packets that it receives. Cryptographic techniques are used to protect the physically unprotected mesh routers from various DoS attacks including gray hole and black hole attacks. But if the router is compromised the attacker will gain access to the private/public key pair of the router and can break through the cryptographic systems. Thus non-cryptographic methods will provide a second line of defense [14], [15]. In this work we try to develop a non cryptographic type of defense by checking the forwarding of the upstream routers by overhearing their transmission. We consider AODV routing protocol to implement these attacks.

3.1 Ad-hoc On-Demand Distant Vector (AODV) routing protocol

AODV protocol is one of the commonly used in wireless mesh networks and is proposed as one of the protocol in the IEEE 802.11s standard [16]. AODV is a reactive distance vector routing protocol which will establish the path only when the

router has some data to send. AODV borrows the basic route establishment and maintenance mechanisms from the Dynamic Source Routing protocol (DSR) and the hop-to-hop routing vectors from the Destination-Sequenced Distance-Vector protocol (DSDV). To avoid routing loops AODV makes use of the sequence number in the control packets.

When source node intends to communicate with a destination node whose route is not known it broadcasts a Route Request packet (RREQ). Each RREQ contains an ID which uniquely identifies the RREQ packet, source and destination IP addresses and sequence numbers together with the various control flags. The sequence number maintains the freshness of the control messages and the hop count maintains the number of nodes between the source and the destination. On receiving a RREQ message by the intermediate or neighboring node that has not seen a source IP and ID pair or which doesn't contain a fresher route (larger sequence number) to destination will rebroadcast the packet after incrementing the hop count. Such intermediate nodes will also create a reverse route to the source node for a particular interval of time.

When the RREQ reaches the destination node or any intermediate node which has a fresher route to the destination a Route Reply (RREP) packet is generated and unicast backward to the source of the RREQ. Each RREP contains the destination sequence number, source and destination IP addresses route life time and the hop count together with control flags. Each intermediate node receiving a RREP packet will increment the hop count and establishes a forward route to the source of the packet and send the RREP packet in the backward route. A Route Error (RERR) packet is send by a node to its neighboring nodes if there is a link break observed in the active route. Once the route is updated by all the nodes the source will send packet to the destination in the route.

When using AODV in multiple radios in a node, the RREQ is broadcasted on all the interfaces of the node. In order to avoid broadcast storms each RREQ is send after a random time interval. Intermediate node with more than one interfaces and working on a channel will receive the RREQ and create a reverse

route to the source of the packet. If the RREQ is a duplicate it is simply discarded. The first RREQ received by the destination or an intermediate node having route to the destination is selected and all the other RREQs are discarded. Then RREP is generated for the selected RREQ and is send back to the source of the RREQ in the reverse path.

3.2 Black hole attacks

In a black hole attack the malicious node will always advertise in the network that it has a fresher route to the destination by setting the sequence number to a large value and will reply to the RREQ before other routers send a reply. Thus the attacker router will attract all the traffic in its transmission range towards itself and then may drop the packets [17].

3.3 Gray hole attacks

In a wireless mesh network that uses AODV protocol one attacker node can drop some selected packets according to some criteria or randomly. This is called gray hole attack or selective drop attack. This type of attack is very difficult to detect, especially in the wireless scenario, because packets can be dropped because of line congestion, channel capacity, etc. In the simulation we used random dropping of packets using the random function. While the packets are sending to destination, packets are dropped randomly by the malicious node. Simulation of gray hole attack is done on ns-2.34 [18]. In order to simulate gray hole attack on ns2 we had to modify and implement the existing AODV protocol.

3.4 Implementing the new Routing Protocol in NS-2 which show Gray hole behavior

Implementation of the gray hole attack is done in AODV protocol and simulated in NS-2.34. To show the gray hole behavior, one node is selected as attack node and it will drop packets randomly. The attack node should be able to participate in

```
#GAODV patch
Simulator instproc create-gaodv-agent { node } {
        #  Create GAODV routing agent
        set ragent [new Agent/gAODV [$node node-addr]]
        $self at 0.0 "$ragent start"      ;# start BEACON/HELLO Messages
        $node set ragent_ $ragent
        return $ragent
}
```

Figure 3.1: $ns - lib.tcl$ GAODV modifiation

the AODV messaging. For this the new protocol which exhibits gray hole attack should be able to participate in AODV messaging. Implementation of the new routing protocol which perform gray hole attack is explained below.

All routing protocols in NS2 are installed in the ns-2.34 directory. We start by duplicating the AODV protocol in this directory and named the directory as "GAODV "(all the header files and classes of AODV directory are modified).

All the files in the AODV directory are modified with GAODV such as *gaodv.cc*, *gaodv.h*, *gaodv_rqueue.cc*,*gaodv_rqueue.h* etc except for "*aodv_packet.h*. The new protocol will use the same aodv packets and thus its possible for the new GAODV protocol to send the same AODV packets. So we have changed all the names of classes, structures, functions in all the files except for the struct names that belong to the AODV *packet.h* code. By creating all this we have designed aodv and gaodv protocols to send packets with each other. To integrate the GAODV protocol to the NS2, two common files has to be modified. Since we are using the same packets used in AODV, we don't have to modify the common files related to packet. Thus had to modify two files [18].

The first modified file is the $ns - lib.tcl$. It's in this file the protocol agents are coded in a procedure. So here we had to add the protocol agent for the newly created GAODV protocol. When a node is using GAODV protocol this agent is scheduled at the beginning of the simulation and is assigned to the nodes which use the protocol.

The next file to be modified is the $ns - agent.tcl$. In this we have to set the port numbers for the new routing protocol. *sport* is the source port and *dport* is the destination port.

```
#GAODV patch
Agent/gAODV instproc init args {

        $self next $args
}

Agent/gAODV set sport_   0
Agent/gAODV set dport_   0
```

Figure 3.2: $ns - agent.tcl$ GAODV modification

```
gaodv/gaodv_logs.o gaodv/gaodv.o \
gaodv/gaodv_rtable.o gaodv/gaodv_rqueue.o \
```

Figure 3.3: $makefile.in$ GAODV modification

The third file modified is the $makefile.in$ in the root directory of ns-2.34. This file is modified for creating the object files for the cpp coded files. After all the implementations are ready, we have to recompile NS-2 again to create the object files.

Till now we have implemented a new routing protocol in NS-2 which is labeled as GAODV. But we still didn't implement the gray hole attack in this protocol. As of now this protocol will act similar to the AODV protocol. To add gray hole behavior in to the new protocol we made we had to make some changes in the *gaodv.cc* C++ file. By explaining the working mechanism of AODV and GAODV protocol we will describe the changes made to the *gaodv.cc*.

In *aodv.cc* code when a packet is received it is received by a function called the *recv* and the received packets are processed based on the type of the packet. In this code the different control packets in AODV like RREQ, RREP and RERR packets are processed by different functions. The *recv* function checks whether the received packet belongs to any of these control packets. If it so then it will call the *recvAODV* function. If the received packet is a data packet, usually

```
//If destination address is itsself
if ( (u_int32_t)ih->saddr() == index)
   forward((gaodv_rt_entry*) 0, p, NO_DELAY);
else if ((rand()%6)==3 || (rand()%6)==4 || (rand()%6)==1)
// For grayhole attack in the wireless adhoc network, after giving a true route to demanding
// node, misbehaving node drops some packets according to the random function.
   drop(p, DROP_RTR_ROUTE_LOOP);
```

Figure 3.4: *gaodv.cc* GAODV modification

the AODV protocol will forward the packet to the destination address. But in GAODV protocol the code is modified such that it will drop random packets without forwarding it. This attack is implemented in the *recv* function of GAODV. First the conditions checks whether the packet is destined to itself if it so it will accept the packet, otherwise a condition is checked which is made of random numbers and if the condition becomes true the packet is dropped otherwise it will forward the packet.

3.5 Implementing Black hole behavior

Implementation of the black hole attack as a protocol is similar to that of gray hole attack implementation and the library changes are similar and we used the name BAODV instead of GAODV. The *gaodv.cc* file is modified such that instead of dropping packets randomly it will drop all the packets using if else condition and saved the file as *baodv.cc*.

Chapter 4

Proposed Algorithm

Related Work

Assumptions

Pareameters and Thresholds

Attack Detection Algoritm

Factors influencing the threshold values

Simulation of Gray hole and Black hole attack in ns2

Simulation of the Proposed Algorithm

Comparison of Proposed Scheme with CAD algorithm

Chapter 4

Proposed Algorithm

When a node wants to send a packet it will send the RREQ packet and if it receives a route reply first from a normal behaving node, then everything will work fine. But if it gets reply from an attacker node in which implements selective dropping all the packets will not reach the destination. Some packets will be dropped by attacker node. If the selective dropping attack reduces the delivery ratio drastically an algorithm should be implemented to identify such nodes and prevent them from participating in the data transfer. A RREP from an attacker node can reach the source node earlier than a normal node if it is near to the source node or in other words the shortest path from the source to the destination. In this work we focus on developing an algorithm which focus on single dropping attackers in wireless mesh network and concentrate our study on the stationary routers which are present in hybrid wireless mesh networks.

4.1 Related Work

Most of the prior works related to gray hole attacks were studied in the area of ad hoc and sensor networks. These works can be used in the area of wireless mesh networks too. But since wireless mesh networks are mainly targeting the broadband usage these type of attacks will be more common in wireless mesh networks compared to other two networks. So more research work is needed in the field of security in WMNs. Karlof.et.al [19] proposed selective forwarding attack for the first time in wireless sensor networks and suggested that multi path

forwarding can used to counter the attack. But the algorithm fails to suggest a method to isolate the attacking node and remove from the network. Marti.et.al [20] proposed a technique called Watchdog, in which a node continously monitors the neighbouring nodes to which the packet is sent and to check whether the packet is forwarded or not. But the algorithm fails to detect the attacker in the presence of selective forwarding attack and to completely remove the node from the network. Devu Manikantan Shila.et.al [14], [15] proposed a channel aware detection of gray hole attack based on CAD algorithm in which they observe the forwarding nature of the downstream node as well as the upstream node and detects the attack node. The algorithm works well in the presence of normal channel losses such as wireless medium losses and MAC layer collisions but for identifying the attack, extra packets has to be send by the source node.

4.2 Assumptions

We assume that all the routers that are in the network are stationary and have no energy constraints. We also assume that the wireless interfaces support promiscuous mode operation. Promiscuous mode means that if a node A is within range of a node B, it can overhear communications to and from B even if those communications do not directly involve A. While promiscuous mode is not appropriate for all wireless mesh network scenarios (particularly some military scenarios) it is useful in other scenarios for improving routing protocol performance. We also assume that the each router is provided with an infinite buffer size so that no packets are dropped because of buffer overflow. In the case of black hole attack we assume that the attack node will drop all the packets that it recieves. Finally we also assume that each mesh router is provided with a private/public key pair and also all the public keys of other routers in the network. These keys are used to protect the packets generated while broadcasting the packet reporting the attack generated by the algorithm.

4.3 Parameters and Thresholds

Before going in to details about the algorithm, we introduce the parameters and threshold values used in the algorithm. At each router n_t denotes the number of packets transmitted under a particular threshold to the downstream node. This threshold is denoted as $n_{threshold}$. At the same router n_o denotes the number of packets overheard by the router. n_o can be calculated by overhearing the downstream node to which the data is sent. n_d is used to denote the number of packets dropped by the downstream node. P_a is used to denote the probability of attack by the downstream router and also P_g and P_b are the threshold values called the probability of gray hole attack and probability of black hole attack respectively.*interval* is the number of times the probability of attack is checked with the threshold values in a given interval.

4.4 Attack Detection Algorithm

We present an algorithm for finding the intentional selective dropping attack by a node and if all the packets are dropped will identify the attack as a black hole attack by checking the forwarding of packets by the immediate neighbor downstream node to which the data is sent. For this we have to overhear the traffic by the neighboring nodes.

In our algorithm at each mesh router, the router will maintain a packet count history of the number of packets it has forwarded to the downstream node and also the number of packets it has overheard for the forwarded packets. When a router forwards a packet to the downstream node, the number of packet sent (n_t) is incremented and also buffers the packet for a certain time period. Then it overhears the packet which is forwarded by the downstream node and compares with the packet in the buffer. When a match is found the number of packets forwarded by downstream node (n_o) is increased. Once the match is found or if the time period is over the packet is deleted from the buffer. If the packet forwarding is not heard with in the time period the algorithm assumes that the packet is dropped by the downstream node. After sending out a threshold number

of packets ($n_{threshold}$), the number of packets dropped (n_d) is calculated and is the difference of the number of packets transmitted to the number of packets overheard.

$$n_d = n_t \text{ - } n_o$$

According to these observations each router will maintain a probability value called the Probability of attack (P_a), which is obtained by the number of packets dropped by the downstream node(n_d) to the number of packets forwarded by the router to the downstream (n_t).

$$P_a = \frac{n_d}{n_t}$$

The obtained probability of attack (P_a) is compared with a threshold value of probability called probability of black hole attack (P_b) and if P_a is greater P_b then a possibility of black hole attack is identified.
if $P_a > P_b$, possibility of a black hole attack.
When this condition fails P_a is compared with probability of gray hole attack (P_g), and if P_a is found greater than P_g then a possibility of gray hole attack is identified.
if $P_a > P_g$, possibility of a gray hole attack.
If these conditions becomes true twice with in the *interval* an attack is identified. If P_a becomes greater than P_b twice in the interval then a packet is broadcasted to all the routers in the mesh network by the identifying router with the reporter node id, attacker node id and also the type of attack denoted by 'B'. If P_a becomes greater than P_g twice in the *interval* then a packet is forwarded as before with the type of attack as 'G'. If P_a is greater than P_b and P_g once in the *interval* then the type of attack is 'G'.

At each router they maintain a table called the Attack table. When an attack is reported each router will update its attack table with the reporter node id, attacker node id and also the type of attack. If a router is reporter by two different routers then that is identified as an attack node. In AODV protocol if a node recieves a RREQ it will check in the attack table and will not forward the RREQ to a attack router there by isolating them from the network.

Reporter Node id	Attacker Node id	Type of Attack
Router 5	Router 6	G
Router 2	Router 6	G

Table 4.1: Attack Table

4.5 Factors influencing the threshold values

There are some factors which will influence the threshold values used in the proposed algorithm. They are

- False positives

  False positives will occur when router gives a false alarm when no threat or attack exists.The threshold values should be determined such that the chance of false positives are less and at the same time should detect the attack. The probability of false positives will increase with increase in the *interval* and also when $n_{threshold}$ decreases. A decrease in the threshold probability P_g also increases the probability of false positives.

- Loss Due to wireless channel

  Since mesh routers work in a wireless environment packets can be lost due to the wireless channel. Mesh routers are deployed statically over a long period of time and the loss due to the wireless channel can be computed by observing the historical data. Thus the packet loss probability due to wireless channel can be calculated from the channel parameters [14], [15]. So while determining the value of P_g the packet loss probability should be considered over the interval and P_g should be above this probability.

- MAC layer collisions

  Another form of packet loss in wireless networks is due to MAC layer collisions. The probability of collision should be taken in to account in deciding the value of P_g.

- Failure to overhear transmission

  If an ambigous collision occurs at the listening node while the packet is forwarded the listening node will fail to overhear the transmission and assumes that the packet is dropped. So the probability of failure to overhear transmission should be considered before determining the threshold values.

- Quality of Service (QoS)

  Each network will provide some minimum QoS and this will also affect determining the threshold values. The threshold values should be such that the network should be functioning in the QoS requirements even in the presence of attack routers.

4.6 Simulation of gray hole and black hole attack in ns2

We have implemented the protocol which will implement gray hole attack in ns2. Now we have to do simulate the scenario to check whether the protocol is working properly or not. To test whether the implementation of GAODV is working correctly or not we have created a scenario in which 8 routers are connected initially and checked the data traffic when all routers are using the original AODV protocol. After that one of the routers is set to use GAODV protocol and compared the data traffic in both occasions. As expected the delivery ratio of data is decreased when we use GAODV protocol.

4.6.1 Simulation parameters and Metrics

In our simulation we used the UDP connection instead of using a TCP connection. The motivation behind using UDP ahead of TCP is that, in TCP the protocol will close the connection if it won't get a reply ACK from the destination for the packets send. So if the GAODV protocol is implemented then the TCP will close the connection when the router drops the packet. Thus UDP protocol is used in the simulation in which no acknowledgement is received by the source node for

the packets send. Moreover we were able to count the number of packets sent and received in the simulation because of using the UDP protocol. If the TCP protocol is used the source node will stop the connection if the TCP ACK packets are not received.

We choose a scenario in which 8 routers are connected numbered from node 0 -node 7. A UDP connection is created between the node 2 and node 7 and also between node 5 and node 7 with packets are sent from node 2 and node 5 towards node 7. UDP connection is attached with a Constant Bit Rate (CBR), which created constants packets on the UDP connections. CBR packet size is 1024 bytes long and the packets are generated at an interval of .05s. Node 2 will start sending packets from 0.1s and node 5 will start at 0.2s and continue traffic till 4s. The MAC layer used is $MAC\_802.11$ with a data rate of 1Mbyte. We manually define the position of the routers and no movement is added to the routers, since most of the routers in the hybrid wireless mesh networks are stationary.

4.6.2 Result of Simulation

First we simulated the network with no attack node and checked the delivery ratio of the data sent.Delivery ratio is the performance metric used and is the ratio of the data received by destination to the data sent which is expressed in percentage. In the absence of attack the delivery ratio obtained is 100.Then we introduced a malicious node in the network which will implement gray hole attack and drop packets in a random fashion as explained earlier. Router 6 is selected as the attack router which is in the path of the transmission. Since the node 2 and node 5 is sending UDP packets no acknowledgement is sent back by the destination node 7. The delivery ratio is calculated using the data received by node 7 to the data sent by node 2 and node 5. As expected node 6 drops some packets randomly and the delivery is decreased from 100 to a range of 45-60 as shown in Figure 4.1.

Similarly we implemented the black hole attack to router 6 and checked the delivery ratio and the ratio was coming down from 100 percentage to zero.

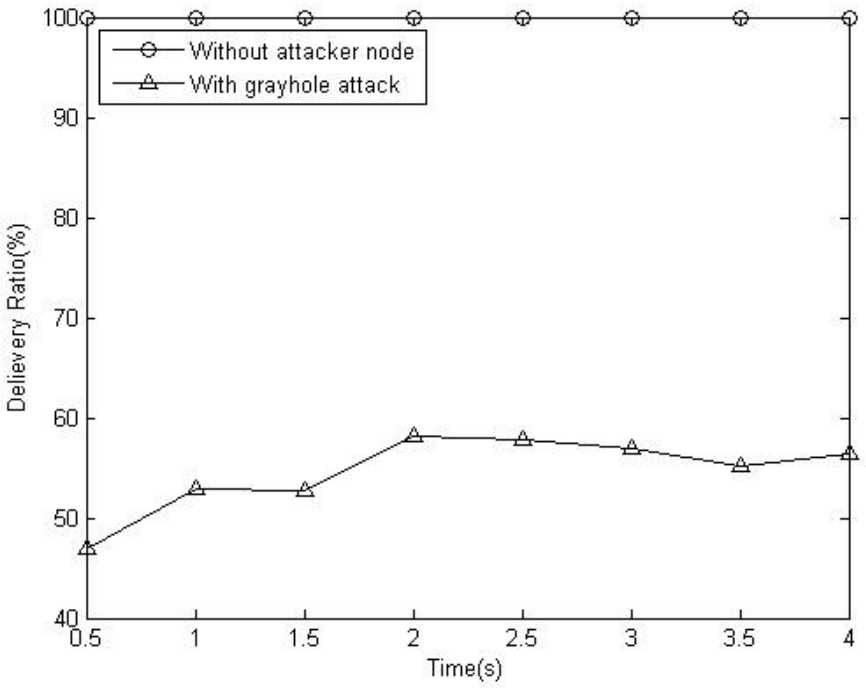

Figure 4.1: Comparison between delivery ratio of network with and without gray hole attack

4.7 Simulation of the Proposed Algorithm

Previously we implemented both gray hole and black hole attack in ns-2.34 and obtained the results. Since we were not able to implement the promiscous mode of operation in ns-2.34 it become impossible to overhear the transmission of the neighbouring router. So we have written our algorithm in Perl language [21] and using the trace files obtained during the previous simulation. Our algorithm will take the trace file as input. Since we are not using simulator for the evaluation of the algorithm, some assumptions are taken while evaluating the algorithm. We assume that once the attack is detected by the neighbouring routers, no time is required for the packet reporting the attack to reach the source and to establish a new path to the destination. This assumption is taken because once we detect the attack in the router we assume that all the remaining packets are routed towards the destination without any drop.

First to determine the value of P_g we started sending packets from router 0 to

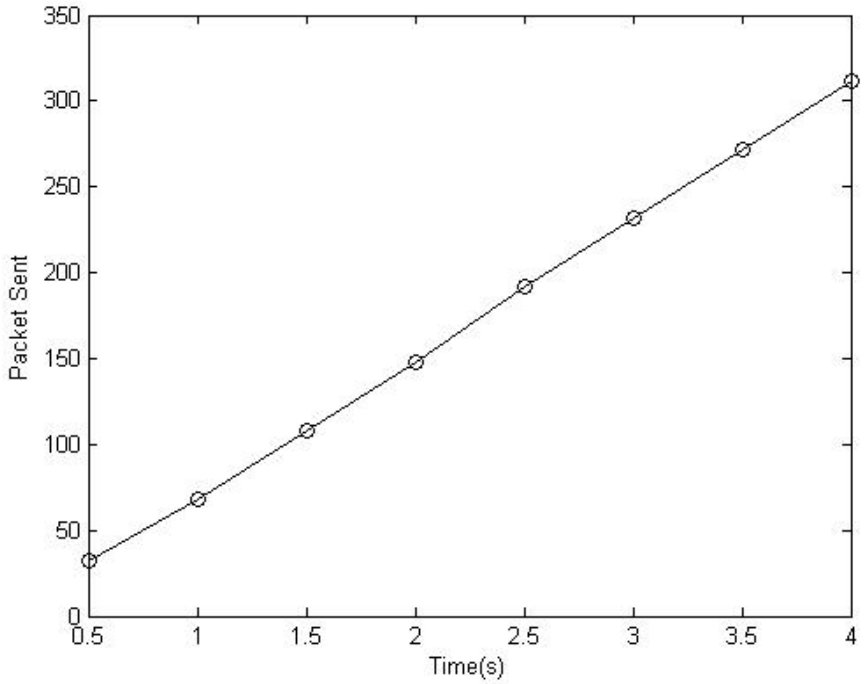

Figure 4.2: Packet sent

router 7 with router 6 as attack node and the delivery ratio drop was from 100 to 60-75. Thus we checked the algorithm with different values of P_g and P_g=.35 was giving a good result when the value of $n_{threshold}$=10 and $interval$=5 and P_b=0.9. These threshold values were used in each neighbouring router and evaluated the performance of the algorithm in the presence of both gray hole attack and black hole attack.

In the graph in Figure 4.4, the value of $n_{threshold}$ is taken as 10. That means the probability of attack is checked after sending out each 10 packets. Since the *interval* is given as 5 if the probability of attack (Pa) goes above the threshold Pg=.35 twice with in 5 checks, a gray hole attack is identified. We assume that once the attack is detected the source router will send a new Route Request and a new path will be established from source to destination.

Similarly the black hole attack router also is identified with the value of P_b set to 0.9. By the proposed algorithm we can observe from Figure 4.5 that the delivery ratio is considerably increased.

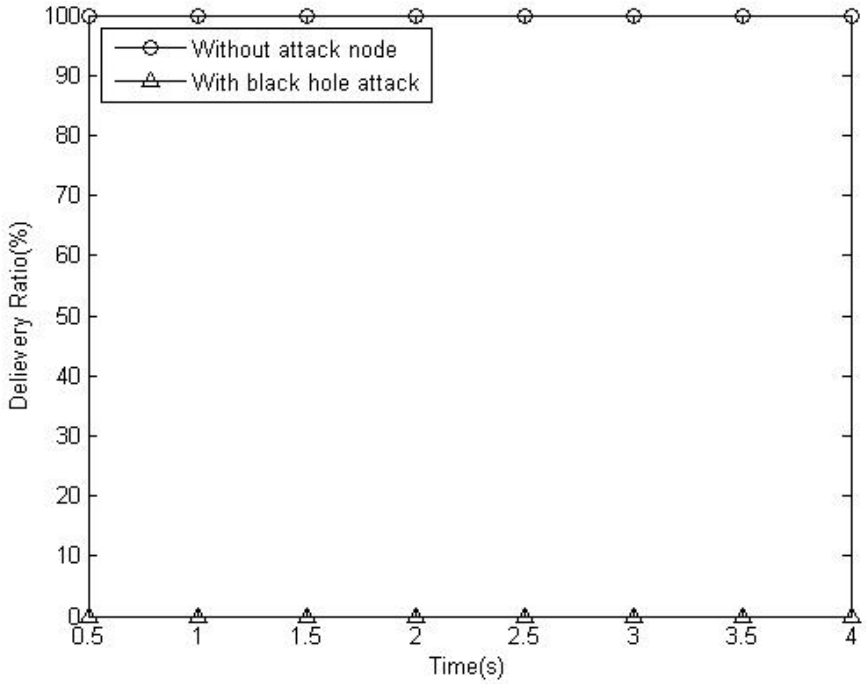

Figure 4.3: Comparison between delivery ratio of network with and without black hole attack

4.8 Comparison of Proposed Scheme with CAD algorithm

CAD Algorithm	**Proposed Algorithm**
Attack detection is done by the source router	Detected by the neighboring routers
Needs to sent extra packet to initiate the detection	No need of extra packets for initiating the detection algorithm
Attack node is identified only if the source router demands	Attack will be reported if a neighboring node observes misbehavior
Threshold values are dynamic and thus changes according to channel behavior	Threshold values are static and performance is less in sudden channel behavior changes
Detection doesnt depend on the data traffic through a node	Higher the data traffic over a network higher the chance that algorithm can detect the attacker
Works well under dynamic channel behavior	Works well under static channel behavior

Table 4.2: Comparison of proposed algorithm with CAD

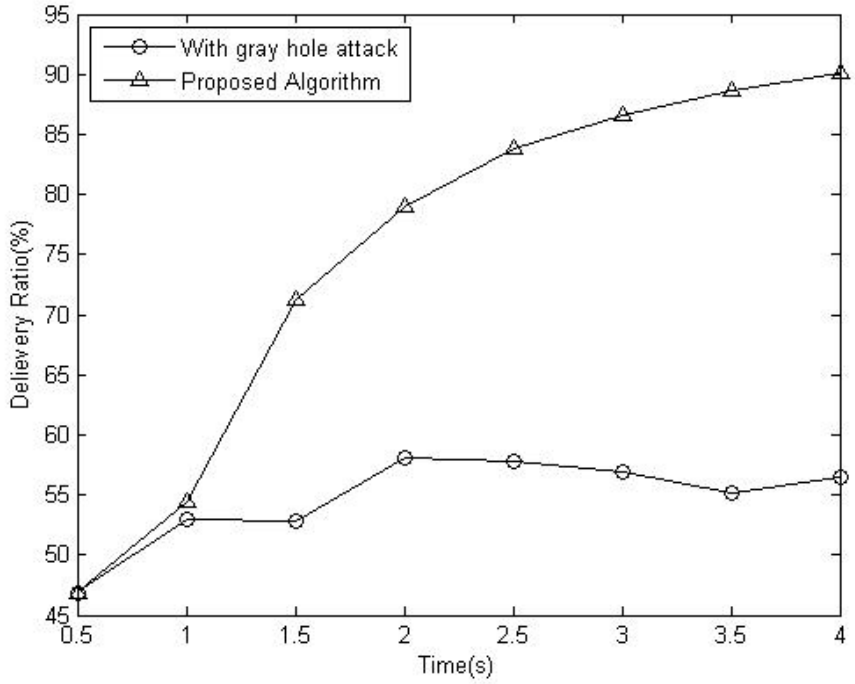

Figure 4.4: Comparison between gray hole attack and proposed algorithm with P_g=.35, $n_{threshold}$=10,$interval$=5

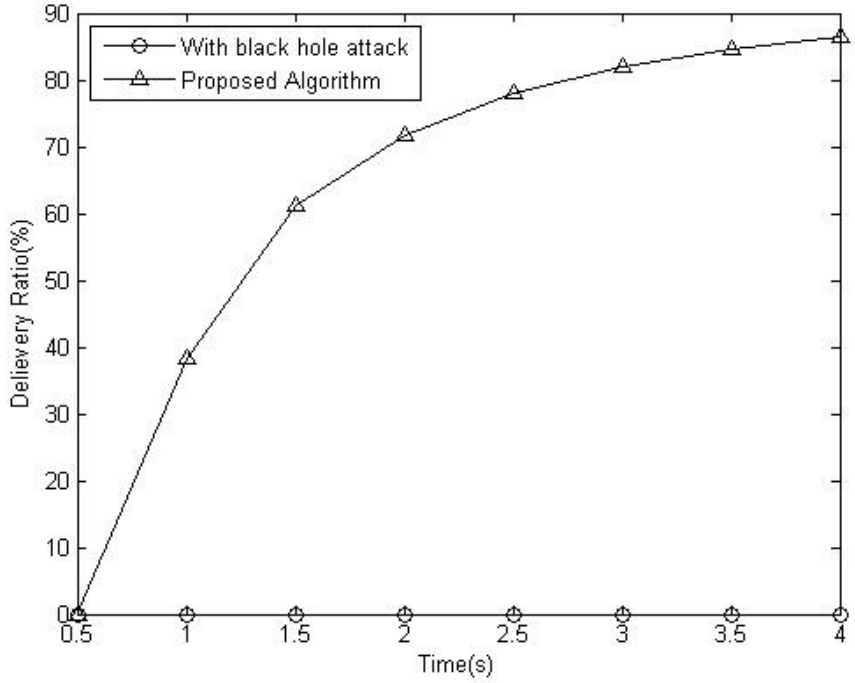

Figure 4.5: Comparison between black hole attack and proposed algorithm with P_b=.35, $n_{threshold}$=10,$interval$=5

Chapter 5

Conclusions and Future Work

Conclusion and Future Work

Chapter 5

Conclusion and Future Work

5.1 Conclusion and Future Work

In future we plan to make the threshold values dynamic in the presence of normal loses due to wireless channel and MAC layer collisions and to work on the attacks when the attack routers collude together.

Since routers in WMNs work in a fully wireless environment the packet can be lost due to different factors. So finding an appropriate threshold value for detecting the gray hole attack in real environment is really difficult. Wireless mesh networks is having an open architecture and more prone to Denial of Service attacks due to its use in broadband internet access.Thus more research work has to be done to reduce the Denial of Service attacks and improve the network.

Bibliography

[1] I.F. Akyildiz and Xudong Wang. A survey on wireless mesh networks. *Communications Magazine, IEEE*, 43(9):S23 – S30, sept. 2005.

[2] Shafiullah Khan, Kok-Keong Loo, Tahir Naeem, and Mohammad Abrar Khan. Denial of service attacks and challenges in broadband wireless networks.

[3] L. Santhanam, D. Nandiraju, N. Nandiraju, and D.P. Agrawal. Active cache based defense against dos attacks in wireless mesh network. In *Wireless Pervasive Computing, 2007. ISWPC '07. 2nd International Symposium on*, feb. 2007.

[4] S. Ghannay, S.M. Gammar, F. Filali, and F. Kamoun. Multi-radio multi-channel routing metrics in ieee 802.11s-based wireless mesh networks and the winner is;. In *Communications and Networking, 2009. ComNet 2009. First International Conference on*, pages 1 –8, nov. 2009.

[5] Choong Seon Hong Muhammad Shoaib Siddiqui. Security issues in wireless mesh networks. In *International Conference on Multimedia and Ubiquitos Engineering*. IEEE Computer Society, IEEE, 2007.

[6] D. Makaroff, P. Smith, N.J.P. Race, and D. Hutchison. Intrusion detection systems for community wireless mesh networks. In *Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on*, pages 610 –616, 29 2008-oct. 2 2008.

[7] S. Seth and A. Gankotiya. Denial of service attacks and detection methods in wireless mesh networks. In *Recent Trends in Information, Telecommunication*

and Computing (ITC), 2010 International Conference on, pages 238 –240, march 2010.

[8] M. Arora, R.K. Challa, and D. Bansal. Performance evaluation of routing protocols based on wormhole attack in wireless mesh networks. In *Computer and Network Technology (ICCNT), 2010 Second International Conference on*, pages 102 –104, april 2010.

[9] M. Medadian, M.H. Yektaie, and A.M. Rahmani. Combat with black hole attack in aodv routing protocol in manet. In *Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on*, pages 1 –5, nov. 2009.

[10] A. Patcha and A. Mishra. Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. In *Radio and Wireless Conference, 2003. RAWCON '03. Proceedings*, pages 75 – 78, aug. 2003.

[11] L. Lazos and M. Krunz. Selective jamming/dropping insider attacks in wireless mesh networks. *Network, IEEE*, 25(1):30 –34, january-february 2011.

[12] D.M. Shila and T. Anjali. Defending selective forwarding attacks in wmns. In *Electro/Information Technology, 2008. EIT 2008. IEEE International Conference on*, pages 96 –101, may 2008.

[13] Guorui Li, Xiangdong Liu, and Cuirong Wang. A sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks. In *Networking, Sensing and Control (ICNSC), 2010 International Conference on*, pages 554 –558, april 2010.

[14] D.M. Shila, Yu Cheng, and T. Anjali. Mitigating selective forwarding attacks with a channel-aware approach in wmns. *Wireless Communications, IEEE Transactions on*, 9(5):1661 –1675, may 2010.

[15] D.M. Shila, Yu Cheng, and T. Anjali. Channel-aware detection of gray hole attacks in wireless mesh networks. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1 –6, 30 2009-dec. 4 2009.

[16] Myung J.Lee and Jianliang Zheng. Emerging standards for wireless mesh technology. *IEEE Wireless Communications*, April 2006.

[17] A. Prathapani, L. Santhanam, and D.P. Agrawal. Intelligent honeypot agent for blackhole attack detection in wireless mesh networks. In *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on*, pages 753 –758, oct. 2009.

[18] K. Fall and K. Varadhan. *NS notes and documentation*. The VINT Project, UC Berkely, LBL, USC/ISI, and Xerox PARC, 1997.

[19] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293 – 315, 2003. Sensor Network Protocols and Applications.

[20] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 255–265, New York, NY, USA, 2000. ACM.

[21] Perl tutorial. www.perltutorial.org.